William & Mary Bill of Rights Journal

Volume 26 | Issue 2 Article 4

The Investigative Dynamics of the Use of Malware by Law Enforcement

Paul Ohm

THE INVESTIGATIVE DYNAMICS OF THE USE OF MALWARE BY LAW ENFORCEMENT

Paul Ohm*

The police have started to use malware—and other forms of government hacking—to solve crimes. Some fear coming abuses—the widespread use of malware when traditional investigative techniques would work just as well or to investigate political opponents or dissident speakers. This Article argues that these abuses will be checked, at least in part, by the very nature of malware and the way it must be controlled. This analysis utilizes a previously unformalized research methodology called "investigative dynamics" to come to these conclusions. Because every use of malware risks spoiling the tool—by revealing a software vulnerability that can be patched—the police will always encounter constraints and disincentives to widespread and unchecked use. These constraints will operate much like so-called legislative "superwarrant" requirements, which some have urged Congress to enact for malware. The investigative dynamics of malware suggest that Congress could follow this advice without disrupting police conduct in any significant measure.

* Professor of Law, Georgetown University Law Center. For helpful comments, thank you to Steve Bellovin, Ahmed Ghappour, and the participants of the Northeast Privacy Workshop and, in particular, Sarah Lageson. Thank you to Roya Butler for research assistance. Thank you also to Adam Gershowitz and the staff of the *William & Mary Bill of Rights Journal*.

INTRODUCTION

From February 20 to March 4, 2015, the FBI infected hundreds and maybe thousands of computers with malware, a computer virus designed to help uncover the identity of people who had configured their computers precisely to avoid being identified.[1] The FBI suspected all of the targets of the malware of accessing a website called PlayPen, purportedly the single largest repository of child pornography online at the time.[2] The malware fulfilled the FBI's intended purpose, leading to hundreds of arrests in the United States and hundreds of referrals to foreign law enforcement partners.[3]

The PlayPen case illuminates more than any before it the increasing use by law enforcement of malware—and other forms of government hacking—as an investigative tool.[4] The use of malware is sometimes necessary, the FBI contends, to bring to justice people who use encrypted services such as Tor and Tor-hidden services—the heart of what is colloquially called the darknet or dark web—who cannot otherwise be identified, arrested, or deterred.[5]

---

[1] *See* United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *1–3 (W.D. Wash. Jan. 28, 2016) (describing the FBI's use of a network investigative technology (NIT) to access computers users had configured to mask identifying information); *see also* Joseph Cox, *Lawyers: FBI Must Reveal Malware for Hacking Child Porn Users or Drop Its Case*, VICE: MOTHERBOARD (Apr. 25, 2016, 7:35 PM), https://motherboard.vice.com/en_us/article/ezpvp4/fbi-playpen-malware-NIT-Jay-michaud [https://perma.cc/FW7V-Y4QQ] (describing NIT as malware).

[2] *Michaud*, 2016 WL 337263, at *1.

[3] Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, VICE: MOTHERBOARD (Jan. 22, 2016, 2:01 PM), https://motherboard.vice.com/en_us/article/qkj8q3/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile [https://perma.cc/WG6R-TEGU].

[4] *See generally* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. (forthcoming Jan. 2018) (manuscript at 1–7) (on file with author) (discussing examples and the rise of government hacking); Cox, *supra* note 1 (describing the government's PlayPen hacking campaign as unprecedented in scope).

[5] *See* Ellen Nakashima, *FBI Use of Hacking Tool to Find Child-Porn Users Affirmed*, WASH. POST, Jan. 30, 2016, at A2 (discussing the FBI's obtaining of search warrants to use

Many law and policy questions arise from the use of malware in criminal investigations.[6] Is the use of malware to obtain a hidden IP address a search under the Fourth Amendment? Will officials abuse malware to spy on political opponents and dissidents? Should the police be allowed to use malware to investigate minor crimes? Should Congress require additional procedures for law enforcement's use of malware?

All three branches of government will be debating questions like these for some time. These tools are too powerful and the application of prior legal rules to them too uncertain to have ready answers to questions like these. This Article hopes to contribute to the coming debates by clarifying what is possible, likely, unlikely, and impossible to occur as the government expands its development, acquisition, and use of these tools.

To do this, the Article also proposes a distinctive research methodology for assessing the impact of technology on policing, criminal procedure, and criminal justice, one that can be extended far beyond malware. This methodology builds on much of my prior work, but particularly on an article entitled *Probably Probable Cause: The Diminishing Importance of Justification Standards*, which looked at how online investigative techniques had diminished the importance of the venerable probable cause standard.[7] I argued that, at least in police investigations of crimes occurring online, almost every new investigative lead comes bundled with probable cause.[8] Unlike the physical world, the online world tends not to produce evidence that seems somewhat suspicious but not enough to establish probable cause, which means that we should no longer think of probable cause as the only tool with which we protected ourselves from unfettered police investigations.[9]

I am formalizing this methodological approach, which I am calling an "investigative dynamics" approach, and applying it to the use of malware by the police. This methodology focuses in particular on how emerging technologies impact policing. It begins with an accurate description of the technology, considered on its own but also in the context of broader societal considerations. It marshals this technological description to try to narrow the scope of what we debate: sometimes fears about what the police or criminals might do with a given technology are unfounded because something—the technology, regulation, institutions, incentives, etc.—render that

---

hacking tools to hack users of child porn); Cox, *supra* note 3 (describing the PlayPen site as being on the "dark web"). *See generally Tor: Hidden Service Protocol*, TOR, https://www.torproject.org/docs/hidden-services.html.en [https://perma.cc/74X4-6B8N] (last visited Dec. 4, 2017); *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en [https://perma.cc/SYW9-6KUH] (last visited Dec. 4, 2017).

[6] *See, e.g.*, Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 26–27, 44–47 (2014) [hereinafter Bellovin et al.].

[7] Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514 (2010).

[8] *Id.*

[9] *See id.* at 1515, 1555–59.

conduct implausible or impossible. The investigative dynamics approach reveals these implausibilities or impossibilities and provides an argument for giving them less attention.

Applied to the emerging government use of malware, investigative dynamics suggests all of the following, none of which I argue has been highlighted prominently in the debate so far. First, the government is extremely reluctant to allow law enforcement to use malware expansively.[10] Malware operates by exploiting vulnerable software, and every use of malware increases the likelihood that a previously unknown vulnerability will be detected and patched.[11] Second, malware is a direct response to the rise of easy-to-use robust encryption, particularly hidden services on Tor.[12] The police will find malware most useful and necessary when surveillance targets are obscuring their identities using technologies like these. Finally, malware must be deployed, monitored, and disarmed to be used.[13] This requires a large technical support team and involves more uncertainty than traditional search approaches.[14]

All of these observations suggest that even absent outside pressure or a new law or regulation, the government is likely to deploy malware primarily in cases involving serious crimes, thorough bureaucratic review, probable cause, judicial review, and when less-invasive surveillance techniques will not work. PlayPen involved every one of these salutary protective steps, and the investigative dynamics suggest that this was not a coincidence. The nature of malware helped bring about these results. We should not preoccupy ourselves too much worrying about hypothetical but implausible uses of malware in the absence of probable cause or judicial review, by uncounseled agents in remote field offices, or to investigate minor crime.

None of this is to say, however, that governments cannot abuse malware.[15] We need some baseline of protection—ideally legislation—to prevent the use of malware for fishing expeditions or to spy on people who are not suspected of committing serious crimes.

The most important implication of this analysis is thus to support new legislation to require more than merely probable cause and judicial review for the use of

---

[10] *See, e.g.*, Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1121 (2017).

[11] *See id.* at 1079–80, 1095–97, 1110–11; Kim Zetter, *Hacker Lexicon: What Is a Zero Day?*, WIRED (Nov. 11, 2014, 6:30 AM), https://www.wired.com/2014/11/what-is-a-zero-day/ [https://perma.cc/ENX4-68TK].

[12] *See, e.g.*, Nakashima, *supra* note 5, at A2.

[13] *See* Mayer, *supra* note 4 (manuscript at 13–18).

[14] *See id.*; *see also, e.g.*, Bellovin et al., *supra* note 6, at 40–41 (describing the government's need for "supporting infrastructure" for operations involving malware).

[15] *See* Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES (June 19, 2017), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html (describing uses by Mexican authorities of spyware to spy on political dissidents and journalists).

malware—what some refer to as a "superwarrant for malware" requirement.[16] The imposition of new superwarrant requirements—such as necessity, intra-agency review, and strict time limits[17]—are necessary to prevent predictable abuses yet will not pose significant barriers to law enforcement operations.[18] They will merely require a judge to require proof of what already seems to be happening—a strictly limited and measured use of malware restricted to important and urgent cases.

Finally, a better understanding of the investigative dynamics will contribute to the "going dark" debate, the roiling public debate about what encryption is doing to law enforcement and what, if anything, can be done about it.[19] The need to use malware will increase with the spread of easy-to-use, strong encryption. But the investigative dynamics suggest that malware will never and can never replace the straightforward investigative tools the police have lost.

This Article proceeds in three additional parts. Part I introduces the investigative dynamics approach to reasoning about the impact of technology on criminal procedure. Part II applies this technique to the use by law enforcement of malware, concluding that structural controls already limit the worst abuses of malware. Part III uses these observations to support legislation imposing superwarrant requirements on the use by law enforcement of malware and to contribute to the going dark debate.

I. METHODOLOGY: STUDYING THE DYNAMICS OF LAW ENFORCEMENT INVESTIGATION

In cases involving the use by law enforcement of powerful new technological tools, we should study how, in the absence of laws regulating their use, the tools are created, disseminated, controlled, and reigned in.[20] Such study will often reveal the investigative dynamics of the tools, which will help us predict how a tool is likely or unlikely to be used. This might give us reason to fear that a tool is susceptible to undetected abuse, which would support calls for external constraints. Or it might

---

[16] *See* Mayer, *supra* note 4 (manuscript at 10, 24–26, 73–78); *see also* Kevin Bankston, *Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors*, LAWFARE (June 14, 2017, 1:00 PM), https://lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors [https://perma.cc/CM4Z-YN9S]; Andrew Crocker, *What to Do About Lawless Government Hacking and the Weakening of Digital Security*, ELECTRONIC FRONTIER FOUND. (Aug. 1, 2016), https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security [https://perma.cc/8SHY-JJ6D].

[17] *See* Mayer, *supra* note 4 (manuscript at 73).

[18] *See* Bankston, *supra* note 16.

[19] *See* BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 1 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/9UDK-PH3H] [hereinafter DON'T PANIC].

[20] I focus on the use by law enforcement of new technology, but this analysis might also apply to the use of new technology by criminals.

lead us to believe that a tool is not so likely to be abused, which would support a wait-and-see approach to regulation and oversight.

A. Probably Probable Cause

In *Probably Probable Cause: The Diminishing Importance of Justification Standards*, I argued that the police tend to build up suspicion in real-world investigations very differently than how they do so in online investigations.[21] In the real world, the police will often gather evidence that is somewhat suspicious but not nearly enough to establish probable cause.[22] Cases like *Terry v. Ohio* build on this observation, creating a sliding scale of search and seizure permitting the police to conduct less than a full-blown search—namely a stop and frisk—with less than probable cause suspicion.[23]

In contrast, I argued that "the Internet is a hunch-free zone," meaning that the evidence gathered in investigations into online crime tend to provide either probable cause or no suspicion at all.[24] I came to this conclusion by focusing on the intrinsic characteristics of the technology, namely "the design of modern communications networks" and "the crucial role played by online intermediaries like telephone and Internet service providers."[25]

The heart of the proof of this claim was a "structural" examination of five features of online spaces and investigations:

> Suspicion builds incrementally in the real world and oscillates between probable cause and nothing online for at least five reasons. First, evidence online almost always comes surrounded by a rich context, providing a high level of built-in suspicion to a suspicious e-mail or IP address. Second, the path from victim back to suspect is fixed and often traceable. Third, the "eye witnesses" online tend to be sophisticated corporate intermediaries without relevant biases or agendas. Fourth, these intermediaries and the victims themselves deploy pervasive systems of surveillance. Fifth, these surveillance systems record precise, unambiguous evidence.[26]

I used these observations to feed back into debates over the proper statutory and constitutional privacy protections to apply in online investigations.[27] Most importantly, the underappreciated irrelevance of justification standards online suggested

---

[21] Ohm, *supra* note 7, at 1515, 1527–28, 1555–59.
[22] *Id.* at 1525–28.
[23] *See* 392 U.S. 1, 10, 20 (1968).
[24] Ohm, *supra* note 7, at 1515, 1529.
[25] *Id.* at 1515.
[26] *Id.* at 1529.
[27] *See generally id.*

the surprising irrelevance of the frequent and roiling debates in Congress over whether to raise the standards for access to stored email in the Stored Communications Act from reasonable suspicion to probable cause.[28] "Because the police almost always have probable cause at every stage of every online investigation, whether we set a requirement at relevance, reasonable suspicion, or probable cause, the police will take every action at exactly the same time."[29]

B. The Investigative Dynamics Approach

Latent within *Probably Probable Cause* was what I recognize now as a distinctive methodology, one worth spelling out more explicitly. The study of the dynamics of law enforcement investigation—investigative dynamics for short—focuses not only on what law enforcement officers theoretically could do, if so inclined, but instead it surfaces what officers will most likely feel compelled to do or not do, given the constraints of incentives, oversight, and—perhaps most distinctively and importantly—technology. This methodology focuses intently on police tradecraft, on an accurate, empirically obtained description of what law enforcement tends to do rather than paying sole attention to what it possibly could do.

The methodology can be used to scrutinize the impact of any technology relevant to police investigations. These might include surveillance technology (like malware), tools operated directly by the police to gather information about targets, whether directly from those targets or from the surrounding environment. Other surveillance technologies susceptible to this analysis would include wiretapping devices, facial recognition systems, and cell-site simulators. The methodology also applies, as in *Probably Probable Cause*, to technologies owned or operated by people other than the police that tend to produce evidence of crime that might be of interest to the police.[30] In that article, I focused in particular on private-operated Internet systems that logged evidence of online behavior, such as web server log files and email headers.[31]

The methodology comprises three steps. First, describe the technology accurately and in as much detail as is necessary to illuminate the next two steps. Second, assess whether features of the technology place or remove direct or indirect constraints or incentives on police behavior. Third, elaborate how these newly surfaced constraints or incentives inform debates about the likely impact or need to regulate the use of technology by police. The three steps focus on the technology, police behavior, and law (and policy), respectively. Consider each step in greater detail.

The first step focuses not on the characteristics of the technology in a vacuum, isolated from broader contexts. Instead, it looks at what many call the socio-technical

---

[28] *Id.* at 1520, 1549.
[29] *Id.* at 1549.
[30] *See, e.g.*, *id.* at 1533–34.
[31] *Id.*

context, although I think that is a bit too grandiose a term for a simple idea: what matters is how the technology fits into pre-existing patterns of human behavior and institutions.[32] In fact, the essential point of the investigative dynamics methodology is to get beyond thinking about what the technology might possibly, conceivably do, irrespective of other constraints, in favor of thinking about what is likely to happen. Some uses are possible but so unlikely to occur as not to merit serious consideration.

Returning to *Probably Probable Cause*, a police officer might conceivably find an email address in the "little black book" of a drug dealer, a scrap of online evidence that might be suspicious but not quite enough to support probable cause.[33] The investigative dynamics approach acknowledges this possibility but argues that this kind of evidence does not turn up frequently enough to displace the general conclusion that email addresses tend to be packaged with enough context to support probable cause.[34]

The second step connects these contextualized characteristics of technology to constraints or incentives on the police. In this step, attention is paid to aspects of technology that make given activities impossible or possible, unlikely or likely. This is perhaps the distinctive move of the methodology, one that borrows from the way technologists and scientists talk about new technology, often analyzing it to conclude how the technology is likely to be used. This kind of thinking does not come easily to non-technologists generally, and legal scholars in particular, who worry about making predictions about technology.[35]

Encryption will often play a key role in this step, as it does in this Article's analysis of malware, even though it did not factor prominently in *Probably Probable Cause*. Encryption, when applied properly, can render the possible impossible and vice versa. For the prognosticator of technology, encryption prunes certain branching possibilities off of the tree of the future.

Finally, step three applies the newly surfaced constraints or incentives to debates about how best to police the police. This step is the practical payoff that connects the assessment of the technology to policy and scholarly conversations about criminal procedure and criminal justice. In *Probably Probable Cause*, because the Internet had reduced the number of incidents in which the police have some suspicion but not quite probable cause, I argued that law enforcement had fewer grounds to object to legislative proposals to amend the Stored Communications Act to require probable cause to read email, for example.[36]

Although this methodology is meant to be precise and rigorous, it is my hope that it can avoid becoming bogged down in terminology or too much formality. I

---

[32] *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 4–6 (2009).

[33] Ohm, *supra* note 7, at 1545.

[34] *Id.* at 1546–47.

[35] *See, e.g.*, Daniel Gervais, *The Regulation of Inchoate Technologies*, 47 HOUS. L. REV. 665, 669, 685 (2010).

[36] *See* Ohm, *supra* note 7, at 1535–42.

intend for this to be a practical methodology, one both scholars and practitioners can utilize. The methodology is also not meant to be applied rigidly. For example, rather than march through the three steps sequentially, we will often bounce back and forth between them.

II. LAW ENFORCEMENT USE OF MALWARE

What are the investigative dynamics of malware? Part I detailed three steps used to assess the investigative dynamics of a particular technology. In this part, I apply the first two steps of the methodology—the characteristics of the technology and the impact on law enforcement—focusing on three aspects of malware. First, malware is a "wasting resource." Second, the need for malware is most compelling in the face of well-implemented encryption, especially on the darknet. And third, malware-aided investigations are a tailored and concerted undertaking. Part III will undertake step three, an analysis of what these newly revealed investigative dynamics of malware mean for many of the law and policy questions that have been raised. Before we begin, let us review what we know about the increasing use by law enforcement of malware.

A. Malware[37]

Until the rise of Tor and the dark web, the use of government malware appears to have been sporadic. For a decade, the only widely acknowledged use surrounded a bomb threat directed at Timberline High School in Washington State in 2007.[38] Commenters have pointed to the use by the government of key logging software, for example, in the investigation of Nicky Scarfo in 1999.[39]

PlayPen marks a significant advance in the use of malware by law enforcement, but it is not a solitary example, as news reports and court dockets are rife with other recent examples.[40]

---

[37] A note on terminology. In the emerging literature on this topic, different authors refer to these bits of code using different names. Jonathan Mayer speaks generically of "government hacking." *See* Mayer, *supra* note 4. Ahmed Ghappour embraces the Justice Department's innocuous-sounding "network investigative technique," or NIT. *See* Ghappour, *supra* note 10, at 1079. Steve Bellovin, Matt Blaze, Sandy Clark, and Susan Landau speak generally of "exploits" but also point to DOJ's mouthful, "Computer and Internal Protocol Address Verifier" or CIPAV. *See* Bellovin et al., *supra* note 6, at 31–32. I, preferring not to mince words, will stick with "malware" or, occasionally, "virus."

[38] *See* Mayer, *supra* note 4 (manuscript at 4–5).

[39] *See, e.g.*, *id.* (manuscript at 5 & n.16); *see also* United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[40] *See* Mayer, *supra* note 4 (manuscript at 14) (discussing "Operation Torpedo" and an investigation into the "Freedom Hosting platform" in addition to the PlayPen investigation, also known as "Operation Pacifier").

Malware is software designed to conduct surreptitious surveillance on a target's computer or network.[41] Jonathan Mayer helpfully identifies four "steps" in the government's use of malware: "delivery, exploitation, execution, and reporting."[42] Rather than reiterate his detailed discussion of all four, consider a few thoughts on each, focusing in particular on aspects highlighted in the discussion below.

To install malware, the police need some method for delivering software to the target's computer.[43] In PlayPen, the government used a so-called "watering hole" technique, taking control of a notorious distribution point for child pornography, but allowing the server to continue to operate, in order to send malware to its users.[44] Some delivery mechanisms are less technical, embracing techniques used in phishing scams or other forms of social engineering.[45] In fact, malware has reportedly been delivered through USB drives left on the ground of parking lots or sold in mall kiosks near the workplaces housing target networks.[46]

The most important of the four steps for this Article's analysis is the exploitation step. Because modern operating systems recognize malware behavior as threatening, malware cannot operate unless it can exploit a vulnerability in the target computer's security systems.[47] Malware thus competes in a multi-party arms race, as operating system vendors seek out the same vulnerabilities and try to eliminate them by distributing patches—small modifications that fix known vulnerabilities.[48] Because there is no such thing, and can never be, as perfect, bug-free code, this arms race is continuously and indefinitely "re-armed" with new, vulnerable code, waiting to be detected and exploited or patched.[49]

Very old malware is therefore usually useless, because it is tailored for old vulnerabilities that no longer exist; patch distribution is difficult to achieve at scale, however, and many computers and networks remain riddled with known vulnerabilities

---

[41] *See id.* (manuscript at 4–5); *see also* Ghappour, *supra* note 10, at 1079–80.

[42] Mayer, *supra* note 4 (manuscript at 13). Ahmed Ghappour divides the activity of government malware into "two steps: access to data and extraction of data." Ghappour, *supra* note 10, at 1096. Mayer's first two steps correspond to Ghappour's first step, and Mayer's last two steps correspond to Ghappour's second. I am using Mayer's framework because it surfaces nuances relevant to my approach.

[43] *See, e.g.*, Mayer, *supra* note 4 (manuscript at 13–15).

[44] *Id.* (manuscript at 13–14, 14 n.41); *see* United States v. Michaud, No. 3:15-cr-05351 -RJB, 2016 WL 337263, at *1–3 (W.D. Wash. Jan. 28, 2016).

[45] Mayer, *supra* note 4 (manuscript at 13).

[46] *See* Bruce Sterling, *The Dropped Drive Hack*, WIRED (June 29, 2011, 12:35 PM), https://www.wired.com/2011/06/the-dropped-drive-hack/ [https://perma.cc/8N6U-RE48].

[47] Bellovin et al., *supra* note 6, at 23–24 (defining "vulnerability" and "exploit"); *see also* Ghappour, *supra* note 10, at 1097.

[48] *See* Ghappour, *supra* note 10, at 1110.

[49] *See* Bellovin et al., *supra* note 6, at 27–28, 30 ("We conclude that for the foreseeable future, computer systems will continue to have exploitable, useful holes."); *see also* Ghappour, *supra* note 10, at 1110–12; Zetter, *supra* note 11.

long after they have been discovered and addressed by patches.[50] A stockpile of old malware might still be useful, if a target has not upgraded to the latest patches.[51] Still, the most valuable and useful malware can exploit a vulnerability unknown to and unpatched by the vendor, sometimes referred to as a "zero-day" or "0-day" vulnerability, referring to the number of days since public discovery.[52]

In the execution step, the malware performs some function on the computer or network it has infiltrated.[53] This often entails rooting around a computer's storage or RAM for incriminating or identifying information.[54]

Finally, malware needs to phone home to law enforcement, reporting what it has learned.[55] Typically, they do so by sending the information back to a police server on the public Internet configured to receive the information.[56]

B. The Investigative Dynamics of Malware

An assessment of the investigative dynamics of the use by law enforcement of malware supports three conclusions that have not before been highlighted prominently. First, malware is treated by the government as a wasting resource, causing it to be subjected to significant constraints and protections. Second, malware is most useful—and most often deployed—to find and watch targets who have protected their activities and communications with robust encryption. Third, the delivery and reporting steps of malware require a sophisticated and complex technological infrastructure operated by technical experts.

1. Malware as a Wasting Resource

What stops the police from using malware indiscriminately? We might feel comforted if we had reason to believe that something constrained the police, making it less likely they would deploy malware without seeking permission from headquarters or to investigative relatively minor crimes.

There are intrinsic characteristics of malware that act like technological checks on government misuse or abuse. To be clear, the government absolutely can abuse

---

[50] *See, e.g.*, Bellovin et al., *supra* note 6, at 50, 54.

[51] *See id.* at 54.

[52] *Id.* at 23; Ari Schwartz & Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process* 1, 3 (Belfer Ctr. for Sci. & Int'l Affairs, Discussion Paper No. 2016-04, 2016), https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf [https://perma.cc/9S27-SQQE]; Zetter, *supra* note 11.

[53] *See, e.g.*, Mayer, *supra* note 4 (manuscript at 16–17).

[54] *See id.*

[55] *See id.* (manuscript at 17); Sam Zeitlin, Note, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U. L. REV. 746, 751–52 (2015).

[56] *See* Mayer, *supra* note 4 (manuscript at 17); Zeitlin, *supra* note 55, at 751–52.

malware by deploying it when it is neither justified nor procedurally vetted. Mexican officials are reported to have sent smartphone spyware to political opponents and civil rights activists, despite promising a vendor to use the spyware only to investigate terrorists and drug traffickers.[57] But the intrinsic characteristics make such abuses less likely and thus should give us some comfort against the untrammeled use.

a. Step One

Most importantly, every piece of government malware should be viewed as a wasting resource.[58] To infect a target computer, government malware must exploit an existing software vulnerability.[59] But vulnerabilities tend to disappear as soon as they are discovered and patched.[60] This is why there is a premium on so-called 0-day or zero-day vulnerabilities, the name given to software flaws that are unknown to the developer of the software and general public.[61] The government (and others) covet zero-days and guard the ones they know about jealously.[62]

Every exploit of a vulnerability hastens the public's discovery and patching of that vulnerability.[63] If the affected target discovers the access to the system that the exploit allowed, he or she is likelier to report or investigate what happened, and thus likelier to bring about the discovery and patch of the vulnerability.[64] In some cases, a copy of the exploit itself can be obtained from an infected machine, giving the malware research community—made up of academic researchers and for-profit antivirus firms—an opportunity to reverse-engineer the code, shedding a light on the vulnerability and possibly even implicating the government in the conduct.[65]

If zero-day vulnerabilities were plentiful, the fact that each was a wasting resource might not matter so much. So long as the government could continuously

---

[57] *See* Ahmed & Perlroth, *supra* note 15.

[58] *See, e.g.*, LILLIAN ABLON & ANDY BOGART, RAND CORP., ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS 52 (2017) (describing the life cycle of vulnerability and exploit).

[59] *See id.* at 2; *see also* Bellovin et al., *supra* note 6, at 23; Mayer, *supra* note 4 (manuscript at 13–17).

[60] *See* ABLON & BOGART, *supra* note 58, at 18; *see also* Schwartz & Knake, *supra* note 52, at 1, 3 ("[D]isclosing information about a zero day vulnerability so vendors can patch it could undercut the ability of law enforcement to investigate crimes, intelligence agencies to gather intelligence, and the military to carry out offensive cyber operations.").

[61] *See* ABLON & BOGART, *supra* note 58, at 2–3; *see also* Zetter, *supra* note 11.

[62] *See* ABLON & BOGART, *supra* note 58, at 2–3, 7–8.

[63] *See* Zeitlin, *supra* note 55, at 750 n.15.

[64] *See* ABLON & BOGART, *supra* note 58, at 52, 58, 66–67; *see also* Zeitlin, *supra* note 55, at 750 n.15.

[65] ABLON & BOGART, *supra* note 58, at 7–8; Ghappour, *supra* note 10, at 1111 ("When a criminal or foreign agent accesses a computer hacked by the United States, he may be able to reverse-engineer the attack in order to use it to attack cyberinfrastructure in the United States.").

obtain new zero-days, most likely by buying them on the open market, it could cope with the risk of loss accompanying each use of malware. The evidence, while incomplete, suggests to the contrary that zero days are extremely rare. Security company Symantec periodically releases statistics about vulnerabilities and exploits.[66] In 2015, it reported that 54 zero-days were discovered, a dramatic increase from the prior years, but still quite small when compared to the number of likely targets of criminal, national security, and intelligence investigations of online activity.[67] One commenter suggests that this number is inflated, because each zero-day is tied to a particular piece and version of software, meaning the number of truly useful zero-day vulnerabilities is likely much smaller.[68]

b. Step Two

These characteristics of information security have given rise to parallel characteristics of government control of the malware it possesses. First, because zero-day vulnerabilities must be hunted for in clandestine settings and jealously guarded once found, the national security and intelligence apparatuses of the government tend to take a central role in these activities.[69] Law enforcement agencies will either borrow malware from their national security counterparts or develop and maintain their own stockpile of malware under strict controls.[70]

Second, the decision to allow malware to cross the transom from the national security to the law enforcement side of the government raises tensions between these two government roles.[71] Most law enforcement activity aims for a public resolution—indictment and conviction in open court. Criminal defendants are entitled to discovery including obtaining information about the investigation that led to their

---

[66] *See, e.g.*, 21 SYMANTEC, INTERNET SECURITY THREAT REPORT (2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [https://perma.cc/9LUB-ABWV].

[67] *Id.* at 5.

[68] Stephen M. Maurer, *A Market-Based Approach to Cyber Defense: Buying Zero-Day Vulnerabilities,* BULL. ATOMIC SCIENTISTS (Mar. 14, 2017), http://thebulletin.org/market-based-approach-cyber-defense-buying-zero-day-vulnerabilities10621 [https://perma.cc/V5W6-RJQH].

[69] *See* Schwartz & Knake, *supra* note 52, at 1–6 (describing government process created to decide how to handle newly acquired software vulnerabilities).

[70] *See id.*; *see also* Ghappour, *supra* note 10, at 1110–11 (discussing inconsistencies between intelligence agencies and law enforcement approach to vulnerability disclosure and malware use).

[71] *See* Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques [https://perma.cc/QXN9-Z3YF] (discussing concerns about the disclosure of secrets through the criminal discovery process).

arrest.[72] When government malware is used to identify a suspect, that fact is sure to be revealed through discovery, if not sooner. The sheer fact that malware was used will often spark an intense hunt in the security community for the vulnerability exploited by the government, hastening the demise of the particular exploit.[73] Even worse for the government, defense lawyers have learned to request the source code for the exploit and to seek judicial compulsion for these requests.[74] For example, in the PlayPen case, at least one magistrate judge has ordered the government to produce the source code, and the government has decided to drop the charges instead.[75]

Third, the role of national security interests or sensitive law enforcement in government assure a federal role in the approval of the use of malware by law enforcement. Despite the vast majority of police conduct that takes place at the state, county, and local levels, malware is likely to remain the province of the Feds. State attorneys general or county district attorneys who want to use malware in criminal cases will doubtless need to coordinate with federal counterparts.[76]

Fourth, within law enforcement, the decision to use malware will likely reside with headquarters and not be left to the field. I and others have written about intra-agency checks on government power in criminal investigations.[77] Summarizing this work briefly, headquarter offices tend to be more conservative and rights-protective than satellite offices in the field, which tend to be more focused on individual prosecutions and less worried about ramifications outside a single case or office.[78]

---

[72] *See* FED. R. CRIM. P. 16; Brady v. Maryland, 373 U.S. 83 (1963) (holding that withholding by prosecutor of any evidence material to guilt or punishment is an unconstitutional violation of due process); *see also* Giglio v. United States, 405 U.S. 150, 153–55 (1972) (holding that withholding evidence of a promise of leniency was material under *Brady*).

[73] *See generally* Schwartz & Knake, *supra* note 52, at 3 (discussing how zero-day vulnerabilities cease to be zero-day when they become publicly known).

[74] *See, e.g.*, Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. May 18, 2016) (order reviewing procedural history of defendant's attempt to compel the government to disclose its N.I.T. code).

[75] Joseph Cox, *Judge Rules FBI Must Reveal Malware It Used to Hack Over 1,000 Computers*, VICE: MOTHERBOARD (Feb. 18, 2016, 5:02 PM), https://motherboard.vice.com/en_us/article/jpgmdg/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud [https://perma.cc/LXS4-ZL8F]; Lily Hay Newman, *The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit*, WIRED (Mar. 7, 2017, 9:00 AM), https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/ [https://perma.cc/72BY-CBQT].

[76] *See, e.g.*, DON'T PANIC, *supra* note 19, at 6 (stating that "state and local authorities have access to fewer resources than law enforcement operating at the federal level"); Mayer, *supra* note 4 (manuscript at 4) (discussing local police cooperation with the FBI in the Timberline High School case).

[77] *See, e.g.*, Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 270–71 (2012).

[78] *See generally* Ohm, *supra* note 77.

In the federal law enforcement system, this division between headquarters and field exist both in the investigative agencies—most importantly the FBI—as well as the prosecutorial arm—main Justice versus the U.S. Attorneys offices.[79] It is impossible to fathom that a single FBI field office will ever be in a position to deploy malware without the full participation of its local U.S. Attorney's office, and it seems inevitable that in every case, both FBI headquarters and main Justice will exert oversight as well. These additional layers of oversight add friction and control and, in the main, make it less likely government malware will be used than if the field office made the decision on its own.[80]

2. Encryption, the Darknet, and Malware

The government's need to use malware to investigate crime is almost always connected to a target's successful use of encryption.[81] A criminal target or suspect who communicates without encryption can usually be tracked without resort to malware.[82] To be clear, even without encryption, targets can hide their tracks—for example, by routing their communications through third-party systems.[83] This is apparently what the teenager implicated in the Timberline High case did, routing his communications through a compromised system in Italy.[84] But the rise of easy-to-use encryption has been a significant catalyst to law enforcement uses of malware.

---

[79] *See generally id.*

[80] *See* Mayer, *supra* note 4 (manuscript at 46) ("[E]xperience with government malware shows that there is not an identity of interests among components of the executive branch.").

[81] *See* Ghappour, *supra* note 10, at 1079 ("Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location."); Mayer, *supra* note 4 (manuscript at 6) ("These privacy and security technologies provide legitimate and important protections. But they also inhibit tried-and-true law enforcement techniques.").

[82] *See* Mayer, *supra* note 4 (manuscript at 6–7); *see also* DON'T PANIC, *supra* note 19, at 1, 4, 7; David E. Sanger, *New Technologies Give Government Ample Means to Track Suspects, Study Finds*, N.Y. TIMES (Jan. 31, 2016), https://www.nytimes.com/2016/02/01/us/politics/new-technologies-give-government-ample-means-to-track-suspects-study-finds.html.

[83] *See, e.g.*, Michael Kassner, *The Dark Side of Anonymous Remailers*, TECHREPUBLIC (Apr. 9, 2012, 12:19 AM), http://www.techrepublic.com/blog/it-security/the-dark-side-of-anonymous-remailers/ [https://perma.cc/B4D9-UZ8F] (discussing "remailers" where a service provider replaces an email address with a pseudonym and sends emails without revealing information).

[84] *See* Mayer, *supra* note 4 (manuscript at 4–5); Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 18, 2007, 12:00 PM), https://www.wired.com/2007/07/fbi-spyware/ [https://perma.cc/FY3M-7L7Z]. Another example of the government's use of malware that did not include Tor, but rather included an IP address that originated from a foreign country, was litigated in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). Magistrate Judge Stephen Smith denied the government's requested warrant in that case. *See id.* at 755.

a. Step One

Before Tor, those who wanted to hide online activity from law enforcement officials wielding warrants and subpoenas faced daunting challenges. They could try to cobble together arcane tools that were not designed to be user friendly, which could be mastered only by those with technical training.[85] If they lacked access to these tools, they were left to resort to easier-to-use but far less robust approaches, such as relying on third-party anonymizers like email remailers.[86] The third parties running those services came under the intense scrutiny of law enforcement officials, and many were forced to cooperate or even had their servers seized.[87] The vast majority of people who wanted to evade government scrutiny turned to solutions such as webmail accounts with mainstream providers like Gmail or Yahoo, which essentially act as little more than speed bumps for the police.[88]

Tor and the darknet significantly recalibrated the arms race between Internet users and government surveillance authorities. Tor came first, providing robust encryption designed to protect the source IP address of Internet communications.[89] The communications from a user using Tor appear to come from another Tor user's IP address, and that user has no way of knowing the true user's IP address.[90]

Just as significantly, Tor has become much easier to install and use since it was launched in 2002.[91] In the early days, users had to install several different components

---

[85] *See generally* Alma Whitten & J. D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 669 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005).

[86] *See, e.g.*, George F. du Pont, *The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils*, 6 J. TECH. L. & POL'Y 175, 191–92 (2001); *see also* Kassner, *supra* note 83.

[87] *See* Press Release, May First/People Link, FBI Seizes Server in Attack on Anonymous Speech (2012), https://mayfirst.org/en/2012/fbi-seizes-server-attack-anonymous-speech/ [https://perma.cc/5TW3-CNQR]; *see also* du Pont, *supra* note 86, at 191–94.

[88] *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 44 (describing widespread use of webmail services which provide limited privacy protection)*; cf.* du Pont, *supra* note 86, at 191–94 (describing the ease with which police dismantle or circumvent remailers); Poulsen, *supra* note 84 (describing a student's use of a Gmail account and a remailer to remain anonymous).

[89] *See* Dune Lawrence, *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built*, BLOOMBERG BUSINESSWEEK (Jan. 23, 2014, 8:51 PM), https://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency [https://perma.cc/ML9W-MPFC]; *see also Tor: Overview*, *supra* note 5.

[90] *See* Lawrence, *supra* note 89; *see also Tor: Overview*, *supra* note 5.

[91] *See* Lawrence, *supra* note 89; *see also* Roger Dingledine et al., *Tor: The Second-Generation Onion Router* (n.d.), https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf [https://perma.cc/BDY4-N2ZP].

in order to use Tor.[92] Each component required tweaking and configuration.[93] Today, Tor comes with an installer familiar to any computer user.[94]

Perhaps of even greater significance are hidden services, which have been part of Tor since at least 2003.[95] Tor can be used to access ordinary web services on the publicly routed Internet and web, but hidden services are designed to be accessible only within the Tor network itself.[96] This reduces points of public visibility even more. For example, when a Tor user accesses a website on the web, that website sees traffic emanating from an IP address, albeit not the user's true IP address.[97]

The more profound effect of hidden services or the darknet is that it empowers those who want to set up repositories of information or channels of communication that are not intended to be discovered by the public.[98] It is tailor-made for small, secret groups of individuals who want to evade scrutiny or notoriety. These groups might serve a salutary purpose—think opponents of authoritarian regimes who want to organize—or an unsavory purpose—think child pornographers or drug traffickers.[99]

b. Step Two

The basic effect of Tor and hidden services on criminal investigations is to render invisible and inaccessible to government searchers the IP addresses of those they are investigating.[100] This significantly disrupts the status quo, because online investigations involving IP addresses have become nearly routine affairs.[101] Even

---

[92] *See generally* Lawrence, *supra* note 89; Dingledine et al., *supra* note 91.

[93] *See generally* Lawrence, *supra* note 89; Dingledine et al., *supra* note 91.

[94] *See What Is Tor Browser?*, TOR, https://www.torproject.org/projects/torbrowser.html.en [https://perma.cc/RD2Y-UZ29] (last visited Dec. 4, 2017).

[95] *See* Lawrence, *supra* note 89; Andy Greenberg, *It's About to Get Even Easier to Hide on the Dark Web*, WIRED (Jan. 20, 2017, 7:00 AM), https://wired.com/2017/01/get-even-easier-hide-dark-web [https://perma.cc/EXN3-NPD6].

[96] *See* Lawrence, *supra* note 89; *see also* Greenberg, *supra* note 95.

[97] *See* Lawrence, *supra* note 89.

[98] *See id.*

[99] *See id.*

[100] *See* Ghappour, *supra* note 10, at 1091–93 ("Use of the dark web by the perpetrator, however, renders these conventional evidence collection methods obsolete. Recall that when someone tunnels though [sic] the dark web to browse a public webpage, his Internet traffic appears to originate from one of thousands of 'proxy' computers rather than the one he is using. Without the ability to obtain a true location for the targeted device, investigators are unable to initiate conventional evidence collection protocols.").

[101] *See id.* at 1090 ("According to the DOJ, use of the dark web by criminals to anonymize communications makes it 'impossible for law enforcement' to pursue criminal suspects." (citation omitted)); *see also* Mayer, *supra* note 4 (manuscript at 6) ("Investigators used to be able to subpoena an Internet service provider for an online criminal's identity; Internet anonymization software makes that impossible. Investigators used to be able to serve a search warrant or wiretap order on a cloud service to obtain a criminal's online communications; end-to-end

small police departments have learned how IP addresses can often lead directly to online intermediaries such as ISPs and web hosting providers, entities that have physical locations and administrators who can feel the pressure of compulsory process.[102] A well-designed hidden service within Tor removes these surveillance pressure points.

The problem is that any crime that can be committed or abetted with Internet technology can migrate to the darknet; to date, most attention has been paid to child pornography, but the infamous market known as the Silk Road was even more notorious as a place to buy drugs.[103] Even though federal agents took down the site in 2013,[104] reports today continue to suggest that drug trafficking on the darknet continues to spread.[105] "Increasingly," says Ahmed Ghappour, "criminals use the dark web to facilitate crimes traditionally conducted in the physical world, such as currency counterfeiting, drug distribution, child exploitation, human trafficking, arms and ammunition sales, assassination, and terrorism."[106]

Malware can thus be seen as a way to make nearly unsolvable crimes solvable. Faced with crime on the darknet, the choices available to the police are limited and cumbersome. If the darknet service provides a method for user-to-user communication, officers can go undercover, hoping to infiltrate a criminal conspiracy and trick targets into divulging identifying information. Given the way online services can enable criminal activity at scale, undercover techniques like these are likely to get at a tiny fraction of criminal behavior. The police can also hope for a lucky break. Luckily, luck seems not to be in short supply. At least three notorious darknet sites have been shut down thanks only to the sloppy behavior of their owners, and the tendency for the Internet to remember everything ever posted online.[107]

---

encryption makes that impossible. Investigators used to be able to seize a criminal's computer and smartphone and search their data contents; device encryption makes that impossible.").

[102] *See* Mayer, *supra* note 4 (manuscript at 4–5); *see also* du Pont, *supra* note 86, at 191–94 (describing remailer administrators succumbing to law enforcement).

[103] *See* United States v. Ulbricht, 31 F. Supp. 3d 540, 556 (S.D.N.Y. 2014); Ghappour, *supra* note 10, at 1077–78; *see also, e.g.*, Cox, *supra* note 3 (discussing the government's unprecedented malware attack in pursuing child pornography crimes).

[104] Kim Zetter, *How the Feds Took Down the Silk Road Drug Wonderland*, WIRED (Nov. 18, 2013, 6:30 AM), https://www.wired.com/2013/11/silk-road/ [https://perma.cc /T569-8HKL].

[105] Nathaniel Popper, *Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail*, N.Y. TIMES (June 10, 2017), https://www.nytimes.com/2017/06/10/business/dealbook/opioid-dark-web-drug-overdose.html.

[106] Ghappour, *supra* note 10, at 1090 (citations omitted).

[107] *See, e.g.*, Ian Burrows, *Alexandre Cazes: Who Was the AlphaBay Founder and How Did Authorities Catch Him?*, ABC NEWS (July 21, 2017, 10:14 AM) (Austl.), http://www.abc.net.au/news/2017-07-21/who-was-alphabay-founder-alexandre-cazes/8730680 [https://perma.cc/QBM6-FKL3] ("It appears Cazes was ultimately brought undone by his own mistake when left [sic] his personal email address visible online."); Alex Hern, *Five Stupid Things Dread Pirate Roberts Did to Get Arrested*, GUARDIAN (Oct. 3, 2013, 4:17 PM), https://www.theguardian.com/technology/2013/oct/03/five-stupid-things-dread-pirate-roberts-did-to-get-arrested [https://perma.cc/KEL2-V8L5]; Graham Templeton, *Dark Market Massacre: FBI*

3. Tailoring, Deploying, and Monitoring Malware

The prior two sections looked at the investigative dynamics influencing whether and when to deploy malware in criminal investigations. Different dynamics implicate how malware must be deployed and controlled, once the decision to do so has been made.

First, unlike the routinized IP address investigation it replaces, each use of malware is far more idiosyncratic and bespoke. Second, malware must be carefully monitored over an extended period of time, requiring a technical support staff and infrastructure.

a. Step One

From what we can glean, the PlayPen virus probably did not exploit a zero-day vulnerability. Popular versions of the Tor software came pre-bundled with the same version of the Mozilla Firefox browser.[108] For some reason, these bundles did not provide an easy-to-use, much less fully automated, patch update system, meaning many Tor users were using an outdated version with well-known vulnerabilities.[109]

Similarly, the FBI's controversial attempts to compel Apple to help it break into the phone of San Bernardino shooter Syed Rizwan Farook turned on the fact that Farook's phone was an iPhone 5c, running a particular subversion of version 9 of the iOS operating system.[110] This fact dictated the possibilities of both the FBI's attempts to guess the phone's passcode—the controversy litigated in federal court—as well as the reported exploit the FBI ultimately used to access the phone—ending the litigation.[111]

Shuts Down Silk Road 2.0 and Dozens More Tor Websites, EXTREMETECH (Nov. 8, 2014, 8:09 AM), http://www.extremetech.com/extreme/193821-dark-market-massacre-fbi-shuts-down-silk-road-2-0-and-400-other-tor-websites [https://perma.cc/5EQT-YHAK] ("[W]eb developer Blake Benthall has been charged with running the Silk Road 2, and if guilty it seems he went down for the exact same reason as . . . Ross Ulbricht before him: he was stupid.").

[108] *See What Is Tor Browser?*, *supra* note 94; *see also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), http://www.wired.com/2013/09/freedom-hosting-fbi/ [https://perma.cc/PX5B-TK63].

[109] *See* Poulsen, *supra* note 108.

[110] *See* Laurie Segall et al., *FBI Says It Has Cracked Terrorist's iPhone Without Apple's Help*, CNN MONEY (Mar. 29, 2016, 9:36 AM), http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html [https://perma.cc/X9WV-8BHL]; Kim Zetter, *New Documents Solve a Few Mysteries in the Apple-FBI Saga*, WIRED (Mar. 11, 2016, 4:01 PM), https://www.wired.com/2016/03/new-documents-solve-mysteries-apple-fbi-saga/ [https://perma.cc/R849-GBZW].

[111] *See* Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points & Authorities; Declaration of Christopher Pluhar; Exhibit, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 16,

These examples highlight a typical pattern when the police use malware. A key step is the selection of precisely the right exploit for the job, one married to the precise version, perhaps down to the sub-sub-sub-version, of the precise piece of software known, or suspected, to be used by the target.[112] "Because exploits must be exquisitely tailored to particular versions and patch levels, using the wrong exploit frequently results in failures, and can even raise alerts or cause suspicious crashes."[113] There is never just one catch-all piece of malware that will work across a broad number of target systems and software versions; the choice of the exploit, the method of delivery, and the techniques used for reporting need to be tailored to each particular case.[114]

Each investigation's tailoring is unlikely to be generalizable to other cases, again because of the wasting resource nature of malware.[115] The next target investigated is unlikely to be running precisely the same version of the same software as the one that worked this time.[116]

In addition, malware requires a large team of technical experts backed by a robust technical infrastructure to operate.[117] Malware needs to be delivered with pinpoint accuracy; for example, in the "watering hole" style of delivery, only those users whose communications match the prespecified indicia of culpability should receive the malware.[118] It might mean that on a large server dedicated generally to pornography, only those who visit a particular forum should receive the malware.[119] Or perhaps it should be sent only to those who attempt to download an image file in a given forum.

Once malware has successfully exploited a vulnerability, it begins to collect information from the target's computer or network, and it needs to transmit that information back to a police monitoring system.[120]

2016); *see also* Complaint, Associated Press v. Fed. Bureau of Investigation, No. 16-cv-1850, 2016 WL 4990082 (D.D.C. Sept. 16, 2016); Segall et al., *supra* note 110.

[112] *See* Bellovin et al., *supra* note 6, at 36–37 ("To remotely access a machine, an attacker generally needs to know the IP and/or MAC addresses of the machine, the operating system (including exact version and patch level), what services are running on the machine, which communications ports are open, what applications are installed, and whether the system contains any known vulnerabilities." (footnotes omitted)).

[113] *Id.* at 36.

[114] *See id.* at 36–37; Zetter, *supra* note 11.

[115] *See supra* notes 38–80 and accompanying text.

[116] *See* Bellovin et al., *supra* note 6, at 33 (explaining how three different targets might require three different exploits).

[117] *See id.* at 40 (describing the need for "supporting infrastructure" including "encrypted channels to the investigators," a "command-and-control subsystem," and "concealment mechanisms").

[118] *See* Mayer, *supra* note 4 (manuscript at 13–15, 61) ("The government may need to impose extra conditions on its watering hole delivery—requiring more than merely visiting the site—to ensure probable cause.").

[119] *See id.*

[120] *See, e.g.*, *id.* (manuscript at 16–17) (describing "execution" and "reporting" in government malware operations).

Sometimes this happens at a single moment of time. Like a search of a home, the point of some malware might be to exploit a vulnerability, deploy some payload that, for example, searches an entire hard drive for certain types of evidence, and "phone home" once with whatever it finds.[121] Like the finite home search, this might take minutes, or even hours or longer to accomplish, but there is a single, discrete moment in the future when the search may be deemed completed.[122]

In other cases, the malware will conduct ongoing surveillance—sometimes it will literally be a wiretapping device such as a packet sniffer or a keystroke logger—and it will reside on the hard drive until it is disabled.[123] It might phone home regularly or even continuously, constantly updating a police dossier of what it has learned.[124] Or it might phone home at one point in the future, uploading a bundle of information acquired over time.[125]

b. Step Two

Because each case presents a unique and idiosyncratic technical situation, and because malware must be carefully deployed and monitored over time, malware investigations will tend to be resource-heavy and hard to standardize into routine investigations.

This does not seem to be a temporary situation. It is likely that the non-routine nature of malware investigation will be true in the near- to midterm. Because of the adversarial, arms race nature of vulnerability and exploit, the police find themselves trapped in a mouse wheel of innovation, forced to throw out the playbook and start fresh with each patch. Short of some major and far-fetched advance in artificial intelligence—a super-tool that can find new vulnerabilities and craft exploits to take advantage of them—this will never become a one-click style of operation.

In addition, malware will require the coordination of a large support team to deploy and monitor. Small, satellite offices, particularly at the state level, where resources might be far more limited than at the federal level, and where technological expertise is often scarce, will find it difficult to support the use of malware.[126] The need to use malware in some types of cases will nudge law enforcement to larger, better supported investigative units and agencies. It takes a police village to use government malware.

---

[121] *See id.* (manuscript at 17).

[122] *See id.* (manuscript at 66–67) (discussing malware cases in which the government requested permission to collect information from the infected computer for thirty days).

[123] *See, e.g.*, *id.* (manuscript at 17) (discussing, in part, malware that remains present and operational on suspects' computers).

[124] *See id.*; *see also* Zeitlin, *supra* note 55, at 751.

[125] *See, e.g.*, Mayer, *supra* note 4 (manuscript at 17, 64–68).

[126] *See* Bellovin et al., *supra* note 6, at 2 (questioning whether local and state law enforcement agencies are capable of developing and utilizing malware); *see also* DON'T PANIC, *supra* note 19, at 6 (describing state authorities' lack of federal resources); Mayer, *supra* note 4 (manuscript at 4–5) (describing local law enforcement's difficulty with malware, thus requiring FBI assistance).

Obviously, nothing prevents smaller units with fewer resources from trying to deploy malware. I predict that smaller units will try to use this tool, but when they do, they will quickly be reminded of why broader support is necessary, as they realize the mistakes they make without support. These mistakes might be revealed during the operation, when the malware they use is detected or directed at innocent bystanders. If not then, they will probably learn their lesson during prosecution, when their methods are challenged or subjected to discovery.

C. Summarizing the Constraints and Incentives

Let us summarize the various "step two" assertions about what the dynamics of malware do to constrain and incentivize police conduct. The decision to use malware will often require consultation with—and even permission from—the national security and intelligence arms of the government.[127] These branches of government are likely to disfavor law enforcement uses, because of the inherently public nature of a criminal prosecution and because of the tools defense lawyers have to force transparency of investigative tools and steps.[128]

These, and other, dynamics will tend to subject requests to use malware to thorough, burdensome, bureaucratic review. These review decisions are likely to involve the headquarters of both the prosecutors and investigators, rather than leave the decision to the field, and will usually necessitate the participation of federal agencies.[129]

All of this bureaucracy and review will disincentivize the routine use of malware. Malware will most often be used in cases involving targets who have hidden their tracks, particularly using robust encryption, and thereby thwarted alternative, less burdensome, routine investigative approaches.

Finally, the need to match exploit to vulnerability across the wide sweep of computer software will prevent malware from becoming a routine process. Every use of malware will feel bespoke and idiosyncratic, giving rise to unpredictable odds of success.[130] Before we turn, in Part III, to how these constraints and incentives clarify various law and policy debates, consider how they contrast with the investigative dynamics of a few other emerging surveillance technologies.

D. Compared to Other Surveillance Technologies

These distinctive features of malware—the idea of a stockpiled exploit as a wasting resource, the role of encryption, and the burdensome and tailored nature of malware investigations—distinguish this class of tools from other seemingly similar surveillance technologies. Let us compare two other technologies reportedly being

---

[127] *See, e.g.*, Mayer, *supra* note 4 (manuscript at 45–48) (discussing interagency surveillance constraints).

[128] *See supra* notes 69–79 and accompanying text.

[129] *See supra* notes 77–80 and accompanying text.

[130] *See* Bellovin et al., *supra* note 6, at 33, 36.

used by law enforcement officials: cell-site simulators (e.g., StingRay devices) and facial recognition software.[131] Very few of the conclusions we draw about malware apply in either of these contexts, supporting the idea that malware presents distinctive issues, concerns, and solutions. Comparing these other technologies to malware further demonstrates the operation (and the power) of the investigative dynamics approach.

Cell-site simulators are designed to masquerade as legitimate telecommunications infrastructure, in a sense "tricking" target cell phones into revealing personal or sensitive information, such as a unique identifier (e.g., IMSI number) or the content of communications.[132]

Cell-site simulators take advantage of the relative openness of cell phone standards. Cell phones rely on publicly available standards promulgated by groups such as the International Telecommunications Union (ITU).[133] One reason standards like these can be spoofed is the need to provide interoperability: a cell phone user does not want her phone calls dropped if the only tower within range is a competitor to her telephone company or when she is traveling internationally. Providers can provide roaming services in those cases, meaning her phone will be willing to at least communicate with towers not provided by her own service.[134]

Cell-site simulators also take advantage of the need for devices to be backwards compatible, meaning capable of communicating with towers using old, outdated standards.[135] This means that even if a cellphone utilizes a harder-to-spoof new standard, say a 4G or even 5G standard, the phone can still fallback to a 2G or 3G standard when that is all a tower appears to support.[136]

These standards dynamics—openness and the ability to force a fallback—differ widely from the "wasting resource" of malware. Cell-site simulators make themselves indistinguishable from legitimate network activity, meaning there is nothing a target can do to avoid the surveillance.[137] This means that law enforcement agents will feel no natural disinclination to using cell-site simulators as often as they are allowed.

---

[131] *See Street Level Surveillance: Cell-Site Simulators*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/sls/tech/cell-site-simulators [https://perma.cc/TS9Y-XG2V] (last visited Dec. 4, 2017).

[132] *See id.*

[133] *See generally Welcome to ITU-R*, INT'L TELECOMM. UNION, https://www.itu.int/en/ITU-R/information/Pages/default.aspx [https://perma.cc/R9UH-LCS7] (last visited Dec. 4, 2017).

[134] *See Understanding Wireless Telephone Coverage Areas*, FED. COMM. COMMISSION, https://www.fcc.gov/consumers/guides/understanding-wireless-telephone-coverage-areas [https://perma.cc/F8VJ-STJ3] (last updated Sept. 8, 2017).

[135] *See generally* Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, WIRED (Oct. 28, 2015, 3:00 PM), https://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/ [https://perma.cc/4338-Q93F].

[136] *See id.*; *see also* Lauren Walker, *Fake Cell Towers Allow the NSA and Police to Keep Track of You*, NEWSWEEK (Sept. 5, 2014, 11:28 AM), http://www.newsweek.com/what-cell-ls-those-ominous-phony-towers-268589 [https://perma.cc/M5EP-TBXW].

[137] *See* Zetter, *supra* note 135.

Next, consider the investigative dynamics of facial recognition.[138] Any image or video captured containing a person's face can be mathematically compared to other images or videos containing faces to search for a match, an indication that the person in both images is the same person.[139] If one of the image sources ties faces to identities, say a registry of driver's license photographs, this is a potent tool for identifying otherwise anonymous people.

The dynamics of facial recognition are more like the dynamics of cell-site simulators than the dynamics of malware in several key ways. Most importantly, there is no structural barrier to the repeated use of the technology.[140]

A key dynamic of facial recognition makes it even more prone to unfettered government abuse than cell-site simulator technology. Every step in facial recognition occurs at a distance, without touching any device belonging to the target.[141] Malware interacts directly with the target's computer, and a cell-site simulator communicates directly with the target's cell phone.[142] In either case, there is a possibility that the affected device will notice, report, or log the government interaction. In stark contrast, once a face is captured—perhaps by a hidden camera—the rest of the interaction happens solely on government systems.[143]

This distinctive dynamic of facial recognition suggests that law enforcement might feel tempted to use the technology even in cases of minor consequence or priority. Divorced from the even somewhat remote possibility that a target will detect the government conduct, there seems to be no intrinsic reason to confine the technology to serious crimes. One can imagine using facial recognition to target nuisance crimes like littering or jaywalking. It's hard to imagine doing the same for cell-site simulator or malware technology. The advantage of the investigative dynamics approach is giving a rigorous methodology to identifying otherwise merely intuitive conclusions like these.

III. IMPLICATIONS

This brings us to what I described as the practical payoff of the investigative dynamics approach—the implications for law and policy debates. Understanding the ideas that malware is a wasting resource, the relationship between encrypted services and law enforcement use of malware, and the burdensome nature of malware

---

[138] *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/CX7V-J9KG].

[139] *See id.*

[140] *See id.*

[141] *See id.*

[142] *See* Ghappour, *supra* note 10, at 1079–80, 1095–97; *Street Level Surveillance: Cell-Site Simulators*, *supra* note 131.

[143] *See* Garvie et al., *supra* note 138.

investigation contributes to many important debates. Every realistic use of malware by law enforcement is a Fourth Amendment search. The focus on investigative dynamics might help the misguided courts who have botched this question realize their errors. Additionally, since the government already adheres to *de facto* procedures resembling so-called "super-warrant" requirements, Congress should consider imposing those requirements *de jure*, imposing a welcome measure of privacy protection without disrupting the status quo much. Finally, malware can never restore what law enforcement has lost in the so-called "going dark" shift to encrypted services.

A. Is the Use of Malware a Search?

Given the technological and bureaucratic conditions described above, courts should understand that just about every use of government malware they will ever encounter must be a Fourth Amendment search, even under a very conservative, government-friendly reading of the applicable cases.

To be clear, I am not making an impossibility proof. Of course the government could use malware to access a computer in a way that would not be deemed a search.[144] But the investigative dynamics explain why they would never feel the need to do so.

Let's clear some ground by taking a few pieces of Fourth Amendment doctrine off the table. First, by definition, the use of malware by the government is an act of self-help, in which the government reaches out directly to the target's account or computer.[145] The government neither makes direct requests of or interactions with third-party intermediaries nor retrieves any information stored by a third party, meaning third-party doctrine cases like *Smith v. Maryland*[146] and *United States v. Miller*[147] are completely inapposite.[148]

Second, under the *Katz* reasonable expectation of privacy test, the subjective prong presents no analytical hindrance to a finding of search in cases like these.[149] By definition, government malware will almost always be used in cases like investigations of the darknet, cases in which the target has expressly sought out and installed software designed to protect privacy and, with the protection of that software, expressly sought out a service configured to protect privacy.

With these prongs out of the way, the essential Fourth Amendment question remaining is the objective prong of *Katz*: is society prepared to accept as reasonable

---

[144] *See* Mayer, *supra* note 4 (manuscript at 54) (describing the government collection of data that is broadcast onto public networks and acknowledging that no warrant is required in such cases); Ahmed & Perlroth, *supra* note 15.

[145] Ghappour, *supra* note 10, at 1079–80, 1095–97; Mayer, *supra* note 4 (manuscript at 39).

[146] 442 U.S. 735 (1979).

[147] 425 U.S. 435 (1976).

[148] *See Smith*, 442 U.S. at 745–46; *Miller*, 425 U.S. at 437–38; *see also* Ghappour, *supra* note 10, at 1079–80, 1095–97; Mayer, *supra* note 4 (manuscript at 39).

[149] *See* Katz v. United States, 389 U.S. 347 (1967); Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015).

an individual's expectation of privacy against exploitation by malware?[150] It is hard to imagine any line of argument that would answer this question in the negative, as the investigative dynamics help us illuminate.

Focus in particular on a piece of information often sought in malware cases: the target's computer's IP address. A target who is not using Tor shares his IP address with every Internet-connected computer he comes into contact with while surfing the web, sending email, or using an app.[151] Decades of law enforcement tradecraft have evolved to make these IP addresses visible to law enforcement investigators without requiring any use of malware whatsoever.[152]

Given the investigative dynamics of malware—the bureaucratic hurdles, interactions with national security agencies, and eventual challenge by criminal defense counsel—no reasonable officer with an ounce of self-preservation would choose the tool when "Ordinary Tradecraft Pattern X" is available instead. The dynamics themselves dictate that almost any malware situation arises precisely because the IP address sought has been hidden away from public scrutiny.

The proper doctrinal category for this kind of government access, then, are those cases that have likened computers to closed containers.[153] Using computer forensics software to analyze the bytes stored on a hard drive or using a packet sniffer to examine the flow of information across a network has constituted a search.[154] So too should courts treat the act of "opening" a computer on the darknet with malware, rooting around that computer's hard drive, and transmitting what is found back to the police, as searches of closed containers, requiring probable cause, a search warrant, and judicial review.

This analysis has led scholars like Orin Kerr and Jonathan Mayer to conclude that the malware in the PlayPen case conducted Fourth Amendment searches.[155] It is of course noteworthy that a few courts have concluded otherwise.[156] But those

---

[150] *See Katz*, 389 U.S. at 361 (Harlan, J. concurring); *see also Smith*, 442 U.S. at 740.

[151] *See* Lawrence, *supra* note 89.

[152] *See* Mayer, *supra* note 4 (manuscript at 6) (describing how law enforcement historically obtained target data).

[153] *See, e.g.*, United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); People v. Gall, 30 P.3d 145, 153 (Colo. 2001); *see also* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 196 (2005).

[154] *See* United States v. Cotterman, 709 F.3d 952, 956–57 (9th Cir. 2013) (en banc) (discussing computer forensic examination as a search).

[155] Mayer, *supra* note 4 (manuscript at 39); Orin Kerr, Opinion, *Remotely Accessing an IP Address Inside a Target Computer Is a Search*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search/?utm_term=.44901f74094e [https://perma.cc/S544-ECLK].

[156] *See* Joseph Cox, *Should Hacking a Tor User to Get an IP Address Require a Warrant?*, VICE: MOTHERBOARD (Sept. 21, 2016, 12:30 PM), https://motherboard.vice.com/en_us/arti

courts are simply wrong. The judges who authored those opinions betray a fundamental misunderstanding of the technology involved, and even some prosecutors have disclaimed relying on their reasoning.[157] Their errors are picked apart well by the work just cited and deserve no further serious attention in this Article.[158]

B. De Facto Superwarrant Protections

Several commentators have recommended the imposition of wiretap-like, superwarrant procedural protections for any use of malware for law enforcement purposes.[159] Congress could enact a new law, for example, perhaps modeled on the Wiretap Act, that required more than the baseline requirements of probable cause and review by a detached and neutral magistrate before the police could be granted a warrant to deploy malware.[160]

Anytime Congress extends obligations beyond merely probable cause and judicial review, it must consider the impact on criminal law enforcement. The study of early malware cases like Timberline High and PlayPen, suggest that law enforcement has already been exercising a *de facto* superwarrant procedure. Supplementing this study with an examination of the technical architecture of law enforcement malware and the bureaucratic safeguards that flow from this architecture suggest that this track record is not merely a coincidence nor the product of self-imposed constraint. It suggests the more tantalizing prospect that these additional procedures and protections are intrinsic, or nearly so, to the use of this kind of investigative tool.

If true, this suggests that a new legislative law imposing some or all of the menu of procedures in the Wiretap Act would be far less than a catastrophe for law enforcement. To be clear, any proposal to impose new procedures is likely to inspire opposition from law enforcement—more oversight and procedures are worse than fewer—but I think this opposition will not be rooted in a well-founded fear of lost cases. Consider three obligations from the Wiretap Act that are typically regarded as important, but onerous: necessity, internal review, and predicate crimes.[161] The government has already imposed forms of all three of these obligations when it has deployed malware in criminal investigations. The analysis of the dynamics suggests that this might be an intrinsic feature of the use of this tool, meaning Congress has less reason to fear the law enforcement impact of enshrining this obligation by statute.

---

cle/ezpq5a/should-hacking-a-tor-user-to-get-an-ip-address-require-a-warrant [https://perma.cc/5LWD-ZSVV].

[157] *See* Kerr, *supra* note 155; Mayer, *supra* note 4 (manuscript at 9, 28, 46).

[158] *See* Kerr, *supra* note 155; Mayer, *supra* note 4.

[159] *See, e.g.*, Bankston, *supra* note 16; Mayer, *supra* note 4 (manuscript at 75–79).

[160] *See* Bankston, *supra* note 16.

[161] *See* 18 U.S.C. §§ 2516, 2518 (2012); Paul Ohm, *The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 491 (David Gray & Stephen E. Henderson eds., 2017).

In the Wiretap Act, the necessity rule requires the officer applying for the super-warrant to provide "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[162] The judge to which the application has been made must "determine[ ] on the basis of the facts submitted by the applicant" the same.[163]

The design of darknet hidden services operates like a particularly fiendish law professor's final exam hypothetical about necessity in a digital age. If the very act of downloading or transmitting content online is illegal, by routing this content through a darknet service, the operators and users of the service are all but ensuring that other investigative approaches would be "unlikely to succeed." That conclusion flows directly from the technological architecture of the darknet.

Once again, I offer no impossibility proof. For virtually any crime abetted by a darknet service, there is a theoretical possibility that the crime might be solvable using a law enforcement technique that does not require the deployment of malware. For example, servers might be misconfigured, revealing the true IP address of the server or a particular user.[164] In fact, the only reason the FBI was able to launch its malware in PlayPen en masse was due to this kind of misconfiguration, which revealed the IP address of the server, but not the individual users.[165]

As another alternative possibility, because the PlayPen server provided a chat-room capability, the FBI could have tried to use conventional undercover techniques to reveal the identity of users.[166] This would have been a far slower, far less likely to succeed approach, one which again would not have worked en masse.

The text and case law relating to the Wiretap Act's necessity requirement suggest that these types of speculative alternatives are not enough to defeat necessity.[167] The text requires only that the alternatives "reasonably appear" insufficient,

---

[162] § 2518(1)(c).

[163] § 2518(3)(c).

[164] The big break in the investigation into the Silk Road website occurred when an IRS agent found an early mention of the website using Google searches traced back eventually to Ross Ulbricht, who was ultimately convicted. *See* Nathaniel Popper, *The Tax Sleuth Who Took Down a Drug Lord*, N.Y. TIMES (Dec. 25, 2015), https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html?_r=0.

[165] Joseph Cox, *An Admin's Foolish Errors Helped the FBI Unmask Child Porn Site 'Playpen*,*'* VICE: MOTHERBOARD (May 16, 2016, 11:00 AM), https://motherboard.vice.com/en_us/article/nz7e8x/an-admins-foolish-errors-helped-the-fbi-unmask-child-porn-site-playpen [https://perma.cc/KK8X-Y4WN].

[166] *See* Ghappour, *supra* note 10, at 1090–95; Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2016, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking/ [https://perma.cc/XQ7Z-54HQ] (detailing the history of FBI hacks).

[167] *See* § 2518(1)(c), (3)(c); *see also, e.g.*, United States v. McGuire, 307 F.3d 1192, 1196–97 (9th Cir. 2002) ("[L]aw enforcement officials need not exhaust every conceivable alternative before obtaining a wiretap." (citing United States v. Brone, 792 F.2d 1504, 1506 (9th Cir. 1986))).

two words that soften the standard in favor of law enforcement conclusions about the alternatives.[168] The standard also excuses officials from even attempting alternatives that reasonably appear "to be too dangerous," which courts have interpreted to include the danger of being discovered.[169]

Congress, of course, is free to write a stricter (or looser) necessity provision in a new statute governing the use of malware. But even if it does, the investigative dynamics suggest the use of malware in darknet cases will be found to satisfy necessity even under a stricter standard: the government has a strong disincentive to use malware except as a last resort.[170] Each use risks revealing a previously undisclosed zero-day vulnerability, destroying the stockpiled exploit, both by releasing the code into the wild and through the operation of the discovery process.[171]

For these same reasons, the government is not likely to be hindered by a new, statutorily mandated requirement of intra-agency review and approval for each use of malware. Congress might again follow the Wiretap Act, which requires the approval of a relatively high-ranking Department of Justice official prior to any application by federal agents of wiretap authorization.[172] Similarly, the same provision of the Wiretap Act restricts the use of wiretaps of wire or oral communications to investigating crimes found on a, admittedly long, list of predicate crimes, such as certain crimes relating to terrorism or drug dealing.[173]

The dynamics of law enforcement malware once again suggest that neither of these requirements would change the status quo for the government, which already exercises *de facto* intra-agency review. In fact, if there are agents or prosecutors in the field who would be inclined to try to use malware without first consulting FBI headquarters or main Justice, they would likely do so against the best wishes of the central authorities. If true, a Congressional mandate might be welcomed by the center of these agencies, as a helpful way to exert control over the periphery.

One factor that headquarters is already likely to consider for each proposed use of malware is the seriousness of the underlying offense. We have at least circumstantial evidence of this, as the cases we know about involve bomb threats and child exploitation, which happen to fall within the crimes defined in the Wiretap Act.[174]

---

[168] § 2518(1)(c).

[169] *Id.*; *see, e.g.*, *McGuire*, 307 F.3d at 1197.

[170] *See supra* Section II.B.1.

[171] *See supra* Section II.B.1.

[172] 18 U.S.C. § 2516(1) (requiring the authorization of "[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General" before an application for judicial authorization to wiretap wire or oral communications).

[173] *Id.*

[174] *See* § 2516(1)(c); *see also* Cox, *supra* note 1; Mayer, *supra* note 4 (manuscript at 4–5).

We have yet to learn of the use of malware in a case that does not involve a crime on the list or that otherwise seems relatively insignificant or petty.[175]

The study of the dynamics of law enforcement's use of malware can give Congress some assurance that the burden on law enforcement of at least some superwarrant requirements will not create an undue burden on the government's ability to fight crime. In the face of arguments made by others—arguments with which I agree but that fall outside the scope of this Article—Congress should strongly consider acting to prevent the abuse of these tools.

C. Malware and Going Dark

This Article's analysis of the dynamics of law enforcement uses of malware can also contribute to the public debate about the impact of the rise of easy-to-use encryption on government surveillance capabilities, commonly called the "going dark" debate.[176]

Most importantly, this analysis confirms what others have already observed: the use of encryption by surveillance targets makes criminal investigation more difficult and less efficient.[177] Because each use of malware comes at the heavy cost of the loss of an investigative tool, and because this cost gives rise to institutional checks both within a law enforcement organization and from other agencies and branches, it is destined to remain an exceptional, "break glass in emergency" sort of tool. It seems implausible that any particular piece of malware will likely become a tool of routine crime fighting.

This suggests that malware can never operate at scale. Each proposed use will be seen as a great burden. Officers will feel great pressure to find ways to make their cases without resorting to malware. This is similar to how many law enforcement agents feel about wiretaps—the superwarrant requirements imposed on them by Title III and state wiretapping laws make wiretaps often not worth the hassle.[178] According to annual reports compiled by the Administrative Office of the United States Courts, law enforcement agents at every level—federal, state, and local—cumulatively apply for no more than 6,000 wiretap orders per year, meaning this kind of authority is sought in a tiny fraction of criminal cases investigated each year.[179]

---

[175] *Cf.* Ahmed & Perlroth, *supra* note 15.

[176] *See* NAT'L ACADS. OF SCIS., ENG'G, & MED., EXPLORING ENCRYPTION AND POTENTIAL MECHANISMS FOR AUTHORIZED GOVERNMENT ACCESS TO PLAINTEXT: PROCEEDINGS OF A WORKSHOP (2016); DON'T PANIC, *supra* note 19; Peter G. Neumann et al., *Inside Risks: Keys Under Doormats*, COMM. ACM, Oct. 2015, at 24, 24–25.

[177] *See generally* Bellovin et al., *supra* note 6, at 30–31; Mayer, *supra* note 4 (manuscript at 6).

[178] *Cf. Wiretap Reports 2016*, U.S. CTS., http://www.uscourts.gov/statistics-reports/wiretap-report-2016 [https://perma.cc/3D8K-6AKH] (last updated Dec. 31, 2016) (reporting 3,168 wiretaps authorized in 2016 and providing historical comparisons).

[179] *Id.*

Malware, then, will never adequately replace what has been lost—the orderly, straightforward sort of online crime investigation that had developed over the past few decades.[180] The victim brings you an IP address, which you type into an online database, which leads you to an ISP, to which you send a subpoena, resulting in a home address, which you ask a judge for permission to search.[181] This type of investigation is straightforward, reproducible, and predictable. It can be boiled down into advice in a police manual or taught in a daylong seminar.

The malware equivalent of this story is far less predictable or orderly. Criminal activity is encountered on the darknet. The police can know neither the identity nor location of the person hosting the service or anybody using the service. If they are lucky, they can gain insight into the software being used by some of the participants—a given operating system, a given browser, or, even better, the particular versions being used. Then, they must obtain precisely the right malware that will work on a vulnerability present in some of that software, which will probably require them to justify the investigation to their headquarters, prosecutor, prosecutor's headquarters, and a judge. After all of this, they will launch the malware, and hope it works.

If anything, this recitation makes the process seem even easier than it is in reality. The PlayPen case was assisted by a few lucky breaks and extraordinary actions: the server was misconfigured for a brief time, revealing a true IP address, which pointed to a server in North Carolina.[182] A foreign law enforcement agency happened to notice this, and was connected well enough to international law enforcement networks to report back to the United States.[183] Even then, the malware reportedly took advantage of the fact that an old software vulnerability in the Firefox browser that had already been patched was not yet fixed in the older versions of Firefox bundled in the Tor browser version that many PlayPen users used.[184] PlayPen required extraordinary effort and some dumb luck. The case would have been impossible without all of this.

Consider a counterfactual: what kind of changes would it require to allow the police to use malware at scale, to come closer to replicating the kind of relatively frictionless investigation that had become easy prior to the spread of strong encryption? Again, the investigative dynamics analysis in Part II can help answer this question. Because malware is a wasting resource, the government would need to

---

[180] Ghappour, *supra* note 10, at 1094 ("With no other leads, the investigation grinds to a halt.").

[181] *See id.* at 1090–95.

[182] *See* Cox, *supra* note 165.

[183] *Id.*

[184] *See* Joseph Cox, *The FBI May Be Sitting on a Firefox Vulnerability*, VICE: MOTHERBOARD (Apr. 13, 2016, 2:25 PM), https://motherboard.vice.com/en_us/article/aekeq4/the-fbi-may-be-sitting-on-a-firefox-vulnerability [https://perma.cc/B7DT-KFHW]; *see also* Joseph Cox, *The FBI Used a 'Non-Public' Vulnerability to Hack Suspects on Tor*, VICE: MOTHERBOARD (Nov. 29, 2016, 11:00 AM), https://motherboard.vice.com/en_us/article/kb7kza/the-fbi-used-a-non-public-vulnerability-to-hack-suspects-on-tor [https://perma.cc/DE5S-LEFQ].

find a steady stream of new vulnerabilities and a way to develop a steady stream of corresponding new exploits. The two ways to do this is to develop them in-house or buy them on the market. In this counterfactual, the FBI would probably need to do both, spending billions of dollars on hiring an in-house virus writing developer corps and enriching the coffers of vulnerability and exploit security firms.

That alone would not be enough. Because malware must be monitored after deployment, the police would likely need to develop a sophisticated process of controlled delivery and monitoring of these tools. Most likely, this would require a centralized technological and bureaucratic infrastructure—perhaps one run out of FBI headquarters. As more criminal activity moved to the darknet, this would mean crime fighting would migrate from state and local police agencies and FBI field offices to centralized control.

Now consider potential risks of police abuse that are exacerbated by all of these necessary structural changes. Our government would employ dozens, if not hundreds, of virus writers. It would underwrite massive new efforts in vulnerability detection. It would centralize power and control of many criminal investigations in FBI headquarters. It would build an unprecedented network of surveillance apparatuses.

You might find some of these to be positive developments. For example, you might see the increased activity in vulnerability detection resulting in an overall increase in cybersecurity.

But I find great risks in this story as well. Because the vulnerability-writing and purchasing activity would be classified, it would shift a significant component of crime fighting into darker shadows. And the centralization of decisions to deploy malware will also concentrate currently dispersed power in one agency's hands.

I thus find much to worry about in the world in which FBI malware becomes a primary tool for law enforcement rather than a last resort. But even those who agree with this assessment might find it an acceptable risk in the broader "going dark" debate for two reasons. First, if the alternative is a mandate for weakened encryption, this might be better. Second, do we really have any choice? Even if the government tries to mandate a weakened encryption standard, unless every government goes along with the mandate, and even then, unless we could enforce these mandates, easy-to-use, strong crypto is probably here to stay.

CONCLUSION

When I first sat down to write about the FBI's use of malware, I expected to write a screed against unchecked and abusive government power. I had written articles like that in the past, and I didn't see why this time should be any different.[185]

---

[185] *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012); Ohm, *supra* note 7, at 1516 ("Congress should instead seek other ways to balance police need with privacy . . . .").

The PlayPen case seemed rich with possibility to expose the massive abuse by the police of a terrifying new technology.

I surprised myself, then, by finding myself less than troubled by what I learned about PlayPen. To be clear, the government abused its power in this case. It is not clear to me that the judge who signed the warrant had power under the Federal Rules of Criminal Procedure to allow this search.[186] The fact that this single warrant was used to effect maybe thousands of searches in computers around the globe seems to strain the Constitution's guarantee that search warrants will be supported with particularity.[187]

But fundamentally, I think the government faced incredible barriers in investigating an important crime, one with truly vulnerable victims. It recognized that the power it sought was exceptional and subjected the novel investigative approach to searching headquarters review. In fact, it checked many of the boxes we would expect the government to need to check if faced with a superwarrant requirement.

The investigative dynamics approach outlined in this Article helps explain what probably led to all of these positive results. Law enforcement agents view malware as a tool of last resort because of the relationship between vulnerability and exploit. The use of malware has been restricted to cases involving serious crimes in which other investigative avenues are likely not available to the police.

While these conclusions might be used to oppose the misgivings of anybody prone to assume the worst from the government's surveillance programs, it also lends support to legislative efforts to cabin these uses. Because the government already subjects itself to superwarrant-like processes, there is little to lose and much to gain through enshrining those processes in law. Because malware could be used to spy on dissidents or political opponents, Congress should ensure a robust judicial review, including importing the Wiretap requirements of judicial and intra-agency review, necessity, serious predicate crime, probable cause, and time limits.

The intrinsic dynamics of malware help keep law enforcement in check in the use of this powerful tool, at least most of the time. We should recognize both that we need legislation to protect the privacy of innocent people in cases where the police might not feel restrained, but also that this legislation can protect privacy without placing much new burden on the police.

---

[186] *See generally* FED. R. CRIM. P. 41(e).

[187] The leading authority on the argument that search warrants for the installation of malware on anonymous Internet hosts may lack particularity is an opinion by Magistrate Judge Stephen Smith, one of the judiciary's most incisive experts on digital search and seizure. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 758–59 (S.D. Tex. 2013).